UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/006,049	12/06/2001	Kin Doe	ADAPP201B	9620

25920 7590 05/24/2005

MARTINE PENILLA & GENCARELLA, LLP
710 LAKEWAY DRIVE
SUITE 200
SUNNYVALE, CA 94085

EXAMINER	
DERWICH, KRISTIN M	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 05/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/006,049	DOE ET AL.	
	Examiner	Art Unit	
	Kristin Derwich	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 December 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☒ Claim(s) *16* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 March 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20 are pending.

Claim Objections

2. Claim 16 objected to because of the following informalities: In line 5 of the claim, there is a word missing, it is assumed the word is "be", in order for the claim to make sense. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Hereafter patent literature that is referenced as prior art will be cited by column and line number in the form of (column number:line number range). For example, the citation (6:23-27) refers to lines 23-27 of the 6th column in the reference.

3. Claims 1-3, 5, 7-10, 17, 18 and 20 rejected under 35 U.S.C. 102(e) as being anticipated by Flyntz, U.S. Patent No. 6,351,817.

As per claim 1:

Flyntz discloses a method for providing a secure computing environment, comprising:

providing an encryption control device, the encryption control device being in communication with a computer and a smart card (5:40-42 wherein the smart card reader functions as the encryption control device);

authenticating a user as a valid owner of the smart card (5:63-66, 6:1-2);

initializing the encryption control device through a challenge/response protocol with the smart card if the valid owner is authenticated (9:48-52 wherein the challenge is the access requests and the response is the stored access privileges on the smart card); and

activating an encryption/decryption engine of the encryption control device to enable access to data in a secure computing environment if the challenge response protocol is executed successfully (9:52-57, wherein enabling access to the second security level functions as enabling access to data in a secure computing environment).

As per claim 2:

Flyntz discloses a method wherein the authenticating a user as a valid owner of the smart card includes providing a personal identification number (5:50-53).

As per claim 3:

Flyntz discloses a method wherein the authenticating a user as a valid owner of the smart card includes providing a biometric identifier (5:50-53).

As per claim 5:

Flyntz discloses a method wherein a biometric scanner is employed for authenticating a user (11:65 wherein the fingerprint reader functions as the biometric scanner).

As per claim 7:

Flyntz discloses a method wherein the smart card stores the user's personal data (5:50-51 wherein the identification information about the card holder functions as the user's personal data).

As per claim 8:

Flyntz discloses a method wherein a personal identification number is used to authenticate a user (5:63-66 wherein the personal identification information used in the comparison is made up of the previously mentioned PIN).

As per claim 9:

Flyntz discloses a method further including, providing control switches for bypassing the encryption control device (5:40-45 wherein the smart card functions as the switch since when it is not detected inside the card reader the card reader, which functions as the encryption control device, is bypassed).

As per claim 10:

A method for activating an encryption control device that is in communication with a computer for providing a secure computing environment for a user, comprising:

providing a card for insertion into a card reader of the encryption control device, the card being configured to receive and pass data (5:60-62 wherein the smart card

must be configured to receive and pass data since it does both during the authentication process);

receiving a biometric identifier from the user, the biometric identifier enabling validation of the user as the authorized owner of the card (5:50-56);

running a challenge/response protocol between the encryption control device and the inserted card, the challenge response protocol establishing that the inserted card and the encryption control device are compatible (9:48-52 wherein the challenge is the access requests and the response is the stored access privileges on the smart card); and

activating an encryption engine of the encryption control device to create a secure computing environment if the user is validated as the authorized owner of the card and challenge response protocol is successfully executed (9:52-57, wherein the second security level functions as the secure computing environment).

As per claim 17:

Flyntz discloses a method for operating a computer in a secure mode, comprising:

providing an encryption control device, the encryption control device (ECD) being in communication with the computer and a smart card (5:40-42 wherein the smart card reader functions as the encryption control device), the encryption control device storing a biometric identifier of a user (5:63-66 wherein the identification information consists of the biometric identifier);

authenticating the user as a valid owner of the smart card, the authenticating further including, receiving a biometric identifier from the user, and comparing the received biometric indicator with the stored biometric indicator for a match (5:63-66, 6:1-2); and

activating an encryption engine of the encryption control device to create a secure operating mode if the user is authenticated (9:52-57, wherein the second security level functions as the secure operating mode).

As per claim 18:

Flyntz discloses a method wherein the ECD includes a storage medium for storing encrypted data (5:23-26).

As per claim 20:

Flyntz discloses a method further including; allowing the user to transfer unencrypted data from a non-secure storage drive (4:60-62 wherein the first security level is unrestricted and non-secure) to a secure storage drive, the secure storage drive storing data in an encrypted format (5:23-26 wherein the second security level stores data in an encrypted format).

Since both levels reside on the same system, if a user has the proper clearances, they could take data stored on the first, unrestricted security level and store it on the second security level thereby functioning as transferring data from a non-secure storage to a secure storage drive.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 4, 6 and 14 rejected under 35 U.S.C. 103(a) as being unpatentable over Flyntz (U.S. 6,351,817) as applied to claims 1 and 10 above and further in view of Davis et al. (U.S. Patent No. 6,088,450), hereafter known as Davis.

As per claim 4:

Flyntz fails to teach a method wherein the challenge/response protocol includes an exchange of private and public keys between the encryption control device and a smart card. However, Davis discloses a method wherein the private key of a token is exchanged with the public key of a security device and the token functions as the smart card and the security device functions as the encryption control device (6:55-65).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include an exchange of public and private keys during the challenge/response protocol because this offers added security to the system as a whole and stronger type of authentication.

As per claim 14, this is another method version of the claimed method discussed above in claim 4 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 6:

Flyntz fails to teach a method further including, monitoring for continued presence of the valid owner; and locking the encryption control device if the valid owner is not detected. However, Davis discloses a method wherein the security device, which functions as the encryption control device, constantly monitors for the valid user and if the valid user is not present then the security device goes into a non-operational state (2:50-57).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to monitor for the valid user in order to ensure that the user did not leave their computer unattended for a period of time, this increases the level of security of the system (2:28-35).

5. Claims 11, 13 and 16 rejected under 35 U.S.C. 103(a) as being unpatentable over Flyntz (U.S. 6,351,817) as applied to claims 1 and 10 above and further in view of Corcoran (Muscle Flexes Smart Cards into Linux).

As per claim 11:

Flyntz fails to teach a method wherein the encryption control device is portable. However, Corcoran discloses a smart card reader, which functions as an encryption control device, that plugs into the computer via USB port, since it can be unattached from the computer, the card reader is independently mobile from the computer and therefore portable (pg. 4, line 1).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to make the encryption control device portable in order to increase its flexibility and use.

As per claim 13:

Flyntz fails to teach a method wherein the encryption control device is hot pluggable. However, Corcoran discloses a method wherein a smart card reader, which functions as an encryption control device, interfaces with a host computer via USB port, thus making it hot pluggable (pg. 4, line 1).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to make the encryption control device hot pluggable because then the host computer would not need to be powered down in order to remove the device after authentication.

As per claim 16:

Flyntz fails to teach a method wherein execution of the challenge/response protocol establishes a secure path between the encryption control device and the inserted card, the secure path allowing for configuration and biometric data from the encryption control device to be transferred to the inserted card and allowing data from the inserted card to downloaded to the encryption control device. However, Corcoran discloses a method wherein a random number is transferred to the card and then encrypted and the encrypted random number is then downloaded to the card reader which functions as the encryption control device (pg. 3 2nd and 3rd bullet).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to create a secure path allowing for information to be transferred to the card and downloaded onto the card reader because if things like private keys are

being transferred from one to the other then a secure path would make the system as a whole more secure.

6. Claim 12 rejected under 35 U.S.C. 103(a) as being unpatentable over Flyntz (U.S. 6,351,817) as applied to claim 10 above and further in view of Clark, U.S. Patent No. 5,815,577.

As per claim 12:

Flyntz fails to teach a method wherein the encryption engine executes RSA public-key cryptosystem. However, Clark discloses a method wherein an encryption module contains an encryption engine that performs RSA encryption (23:39-42).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to execute an RSA public-key cryptosystem because it is well known and difficult to hack into.

7. Claim 15 rejected under 35 U.S.C. 103(a) as being unpatentable over Flyntz (U.S. 6,351,817) as applied to claim 10 above and further in view of Net Warrior.

As per claim 15:

Flyntz fails to teach a method further including; providing a system tray utility program for allowing the user to control and customize encryption control device security features. However, Net Warrior discloses a method wherein a system tray utility program called KillWin allows the user to control the state of the operating system (pg. 2, 3rd paragraph, lines 1-2).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to provide a system tray utility program because this would increase the user's flexibility and control over their security settings.

8. Claim 19 rejected under 35 U.S.C. 103(a) as being unpatentable over Flyntz (U.S. 6,351,817) as applied to claim 10 above and further in view of Novis et al., hereafter known as Novis, U.S. Patent No. 5,728,998.

As per claim 19:

Flyntz fails to teach a method wherein encrypted data is stored on a virtual drive of the computer. However, Novis discloses a method wherein a smart card reader, which functions as the encryption control device, consists of RAM which is a virtual disk and in order to read the virtual disk a virtual drive must also be present (7:26-30).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to store the encrypted data on a virtual drive because it is easier and faster to access the data through a virtual drive.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kristin Derwich whose telephone number is 571-272-7958. The examiner can normally be reached on Monday - Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kristin Derwich
Examiner
Art Unit 2132

KD
KD

GILBERTO BARRON Jr.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100